

Publication Date: 27 July 2023
YSP Podcast Transcript: 372. What are YOU doing about cyber security?

Listen to this podcast episode [here](#).

Intro: Welcome to Your Strata Property, the podcast for property owners looking for reliable, accurate and bite-sized information from an experienced and authoritative source.

Amanda Farmer: Hello and welcome to the podcast. I'm your host, strata lawyer, Amanda Farmer. And my guest this week is Tom Buckley.

Tom is the managing director of All IT Australia and Strata IT, a leading IT service provider. All IT has been operating for over 20 years with the team recently expanding into the specialized cyber security space. Strata IT is a division of All IT with a group of IT engineers who have specific knowledge and experience of the strata industry. The Strata IT division was built from all IT's long track record of serving a number of strata businesses, successfully meeting their unique needs.

Tom is a regular contributor to many ASX listed entities and not-for-profit organization boards, focusing on cyber education. I'll take you right on over now to my chat with Tom Buckley.

Amanda Farmer

Tom Buckley, welcome to the show.

Tom Buckley

Hi, Amanda, good to be with you.

Amanda Farmer

Tom, let us know some of your background, if you have a background in strata or what it was that drew you to strata and how your company Strata IT came to be.

Tom Buckley

Yeah, for sure. So Strata IT is a full subsidiary of AllIT Australia. AllIT Australia has been around for nearly 20 years as a fully fledged, what we refer to ourselves as a managed service provider. And Strata IT has been recently born and created from AllIT. And for a few key reasons, for many, many years, AllIT had worked with a number of many strata managers as their IT services provider covering all facets of IT, which we'll most likely go through later.

And we thought, you know, we've got a team of dedicated engineers in our team, and administrative staff, and a whole range of people that specifically look after strata managers, and we thought, well, this needs its own dedicated company and structure, which we put in place, and those particular engineers that have formed part of Strata IT have been working with strata managers in the IT space for many, many years and know the ins and outs of the programs, the challenges, the larger picture that strata managers face day in day out. So it's been a logical fit and a logical creation for us to move into that area and one that we're very excited about. We've moved our current and existing strata management companies into that entity to service out of there day to day and it's just going from strength to strength.

Amanda Farmer

Tom, why is it so important for strata managers to understand to be across technology and the efficiencies that it brings?

Tom Buckley

Yes, I suppose. Before I answer that, Amanda, the strata industry, I suppose, is obviously a relatively boutique industry. And in terms of IT, I mean, if you look at strata management, you really can't go any longer than a few minutes in one's day without IT. So it's a critical of critical importance. And it's an area that is traditionally been underserved because there hasn't been a dedicated IT firm out there for strata managers.

And obviously it's critical. I mean, if a strata manager, any administrators, administrative staff within those businesses can't access

YSP Podcast Transcript: 372. What are YOU doing about cyber security?

IT, they don't have efficient IT. I mean, there's a whole range of things that we'll go through. Plus the risks of cyber, which is another large area. Then the downtime alone is, is unbelievable and there's not a hell of a lot you can do without effective IT.

So it's also critically important that obviously there's a number of nuances to the strata industry, particularly in regards to IT. There's obviously the large players out there in terms of the platforms, the strata maxes and the property IQs and those kinds of platforms that we look after and working closely with those organizations. And they have their own nuances that a typical IT firm, if they don't know those comes up against challenges and frustrations on the side of the strata manager as well. So we looked to cover all those in a really focused way.

Amanda Farmer

So you've mentioned there some of the unique platforms that our strata managers are using. And look, I really have nothing to do with IT or tech support in our strata management companies, but I do know from working with clients in my legal practice that there are challenges and frustrations that come out of those platforms in particular. So I hear you there. What other tech challenges do our strata managers face commonly?

Tom Buckley

Yes, it's a good one, Amanda, let's park cyber to one side because it's such a large area. But in terms of the other areas, I mean, efficiency is a big one. Obviously, it's such an administrative heavy industry and getting those efficiencies. So we work with strata management companies to look at all the tools and platforms available to them that they may not have heard of or not using effectively. We also see that there's a lot of tools and platforms out there. But are they implemented properly? Are they working properly?

So we do a lot of that work with the administrative teams and the strata managers to get that working properly. Even a lot of work on the hardware side, not only the software side, but the hardware side, having good, well-run, efficient hardware that's running effectively is crucially important as well. And of course, as strata managers, particularly over the COVID period, and the way that particularly meetings with committees and what have you has changed over that period, then that has also changed the way they run meetings, obviously.

So, video conferencing within the office is vitally important because a lot of those meetings are now taking place virtually. So easy use of video conferencing and obviously internet, good quality internet comes into that, good quality facilities come into that, which we look after as well. And then of course, having that ability for strata managers to work from anywhere, obviously more people are in from home, we're now working extended hours, which we do and support extended hours, which is vitally important. Seven days a week is having that flexibility and access is also a very big one. And that's one of the things that strata managers have struggled with in the past, is getting access to their information in a fast and speedy way, I suppose, outside of the office.

A few of the major strata platforms what we refer to as legacy based platforms, which is not necessarily a bad thing, but they are attached to a server, generally in an office. Some of those are moving to the cloud and getting access to those in the past has been a challenge VPN slowness, but there's a number of things that we know just in regards to how we set up the infrastructure and the nuances of each individual platform that we work at and work through to make sure that it's working effectively for each client and each client is different.

Amanda Farmer

And it's not just the owner of the business or the staff of the business who need to access this information that might be stored on a server, is it? It is this unique situation where you also have the clients of that business, the lot owners, from time to time, needing to, wanting to, requesting access to their own records. Right across our country, we have laws in place that allow owners to inspect the books and records of their owners corporation, make appointments with their strata manager.

It wasn't that long ago that we were turning up at strata managers offices and looking at hard copy records. COVID moved everything forward quite rapidly, or at least should have in my view for many strata management companies. And now I see my clients, myself logging in to online platforms to inspect books and records. Do you help management companies with that process,

making sure that is smooth for owners?

Tom Buckley

Yes, there's a few parts to that, Amanda, and 100% yes. There's not only the speed and access and making sure that's set up properly, but there's a few parts to that. There's the logging in component, which is critical in getting that component set up in terms of website and access and all those parts. There's also the security of that. So we look at that and we'll go into the security part, just in particular way in regards to this, that's critical because obviously you're opening up some pretty confidential information in a lot of cases to the internet. So there's a lot of ways that we do an analysis around is it secured and putting the relevant checks and balances in place there.

And the other part of that is the outbound sending of information from strata managers to their clients. And that's critical. And the way we look at that is a lot in regards to the protection of the email platform in the domain. So we've seen a number of instances where strata managers have been spoofed. So just for clarity and information purposes, spoofing is where someone is trying to pretend to be, you know, ABC strata management, for example, and they're not, engaging in a conversation to, you know, financial reasons or whatever it may be to hack either the strata manager or the client, it can happen in a number of ways, but we look at a lot around that as well.

So that outbound and inbound information, I mean, there's a lot of information that is passed around email, and it's a critical area of security that we look at to make sure that's looked at and secured.

Amanda Farmer

Let's have a closer look at cyber security. You've mentioned it a few times now. What are the particular challenges, vulnerabilities that our strata managers have that some of them may not realize they have when it comes to their tech and their cyber security?

Tom Buckley

Yes, for sure. I mean, it's a massive area and rightly so we're seeing an absolute explosion of activity, not good activity in the area from a range of different areas. And I mean, if you just sort of zoom out for a moment and look at why this is, I mean, the people that are attacking businesses are people that are wanting information to use that to their advantage, other financial or holding information to ransom.

And a lot of people say to me, I said, well, you know, "Will it ever happen to me?" And it's an interesting point. I mean, we've seen the Medibanks and the Optises of the world get hacked and they're very prominent and they have to release that information to the market from regulatory purposes and their listed entities and what have you, but we don't tend to find out about the people that have been hacked in small business and medium-sized business, because I mean, people don't really shout it from the rooftops when it occurs.

Now it's an interesting space because what is occurring there is that the federal government is drafting legislation around what is happening for small businesses and it doesn't just rely pertain to strata management businesses but small businesses in general in regards to data leaks and hacks and all those sorts of things.

So there's a big wave of legislation that is coming in terms of what businesses should be getting ahead of and the fines for not being ahead of it. So that's one area. The other area is cyber insurance. A lot of our clients are looking at cyber insurance or having that mandated and the cyber insurance is some time ago it was a tick box exercise, you know, have you got a few things in place or what's the policy, that's now changed and changing rapidly to a much more stringent set of checklists in terms of what has the strata company engaging with someone like us to see, what have they got in place, what are the platforms they got in place, what's their security score, so that's changing big time.

Amanda Farmer

And that the insurer asking these questions before they will agree to provide the insurance.

Tom Buckley

Correct, yes. So it's a balance off between whether they'll even provide the insurance or whether the, obviously how much the policy goes up. So that space is changing really, really rapidly. And the other major space in terms of cyber security, before we get to the intricacies of this particular area, is there's a lot of feedback coming from owners to strata managers, particularly during the proposal stage, if they're taking on a new plan or, you know, at AGMs.

And it's born, it is born out of the fact of the Medibank and the Optus as I mentioned, is how are you dealing with cyber security and my personal information? People are a lot more aware of it and they're asking more questions. And the organizations that we deal with definitely have solid policies and procedures in place, not only internally, but also, you know, really detailed out in a way that they can pass on to their clients to show just how much they are looking after, you know, cyber security and what are the platforms and procedures they've got in place.

So that's sort of where this space has changed. And it's particularly changed over the last few years, but it's really accelerated in the last six months, particularly as I say, as the cyber insurers have really clamped down on that. In terms of, you mentioned how we look at cyber security when we take on a business, we generally do a full rating of the business to see what areas and there's a number of major areas we need to look at in terms of cyber security. There's email and domain security, what we refer to as identity security, so how an individual user connects to the organisation and how they interact with data, how they're sharing out information because as we mentioned, sharing out of information is a big one. Device security, I mean the list goes on, but it is a very tried and proven method of what we look at.

And we bring organizations, generally on a thousand-point scale, but, generally, if you look at it from out of 10, just for simplicity's sake, we generally find that the average strata management company that hasn't had much of a focus on security or they thought they had a what have you, I mean, the average is three and a half out of 10. So it is quite low.

But the good news is, is getting from sort of a three and a half rating to what we would refer to as best practice, sort of eight to nine out of 10. An organization will probably never get to a perfect 10 or a perfect thousand-point score. And there's a number of reasons for that. There's practicality purposes. There's strata managers need to do their job day in day out and we can't lock them down completely. But getting from that low score to an eight and a half, sort of nine out of 10 for best practice is not as onerous as what people think, but it does require specialist's attention and it needs attention, certainly in a concerted effort over a three or four-month period to get them there. And then an ongoing, I mean, as I said, the attacks that we see have gone from somewhat sophisticated to very, very sophisticated and they change day in, day out. I mean, you've only got to look at the amount of exposed programs and things out there that have vulnerabilities in them that we need to patch, etc.

Amanda Farmer

Can you give us an example, Tom, of a strata management company that has been quite vulnerable, whether you're able to reveal a particular scary scenario or just a situation which could have ended up, which could have ended badly if you guys didn't come in and sort out the vulnerabilities?

Tom Buckley

Yes, so we take on a number of businesses that are looking for change in terms of better support and better cyber security, but we also take on a number of businesses that are looking for change because of they've been hacked. And you know, I don't want to fearmonger too much, but I've got a list a mile long of the instances that have occurred.

We've had one instance where a very large supplier has paid a batch payment, well over a hundred thousand dollars. I've got instances well above that as well where email has been hacked, communication has been intercepted, very sophisticated invoices changed, the whole box and dice in terms of you know I couldn't go into a lot of detail, but essentially information has been changed and that payment has been made and unfortunately cannot be recovered.

Now that in that particular instance, they did have a policy, a sideboard policy, but they had actually gone through a bit of a tick boxing exercise and didn't realize that they'd ticked things that they thought they had, but they didn't. So they couldn't lay claim

YSP Podcast Transcript: 372. What are YOU doing about cyber security?

to the policy. I mean, a little bit over a hundred thousand be here to a business, off the straight off the bottom line, not recoverable and that funds have never been able to recover.

So, in answer to that, we took that organization on and no cyber vulnerability, if you look at it, we can't guarantee that a business is going to be fully secure. Because as I say, the landscape is changing so rapidly. I'm talking on an hourly basis, not a daily basis. However, that exact example, that could have easily been stopped by a number of things. Domain security, multi-factor authentication. That particular organization did have multi-factor authentication, but unfortunately they had a method where it was prompting the user a number of times. So we don't use that method as getting into quite specifics, but we take that away because what happened there was that they were getting prompted a number of times and the user thought, "Oh, I better, I better accept this. Something must be requiring it." So they've accepted and let a hacker in. So, it's getting quite advanced in that regard.

Amanda Farmer

What are some of the things Tom that our listeners can or should be looking at now, some action steps that they should be taking to address their cybersecurity?

Tom Buckley

Yes, for sure. I mean, people often say to us, "What are the things we should be looking at in terms of cybersecurity?" And I mean, really, you should be getting in place a trusted IT services provider that knows the industry, because I mean, we can look at sort of 80, 85% of what we do, even in All IT, our parent company in terms of what we do for businesses and 85% applies to the businesses, but there's 10 or 15% that really is specific to strata managers that we should be looking at.

And I've mentioned it a few times, but really securitizing your domain. There's a number of things, I'm getting a little bit tech heavy here, but there's things like DMARC and DKIM, which secure your domain when sending email, TLS and RPT. There's, making sure that your Microsoft secure score settings. I mean, one metric is if you wanted to, if you run the Microsoft platform, the Microsoft secure score, which is something that is provided in the administrative portal of every Microsoft 365, what we refer to as tenancy, which is each company, that gives you a metric of where you're sitting in the Microsoft landscape. And what everyone's using, mostly Windows devices in this industry.

And that's again, a point scoring system that Microsoft uses of the metrics that Microsoft have available, but don't put in place. So Microsoft have a number of things that you can put in place, but don't come in place. They don't come turned on. So they need modification and manipulation to make sure they're applied right for each business and industry. But I mean, we see a lot of those metrics, the Microsoft secure score sitting at 20 to 35%. And again, that should be at least 85%. So, you know, that's a big one.

So people are interested. That's a quick and easy method to find out off your current provider. It'll probably ring alarm bells with the provider if you start asking those questions, but you should know that. And you have the right to know that information. You may not be an administrative user within the tenancy, but you can request that information in a screenshot of it.

Amanda Farmer

And who are you requesting for that information?

Tom Buckley

Generally, whoever looks after your email and in your Microsoft infrastructure, you know, your IT provider, they will generally have access to that. And if they don't, that probably raises more of a flag or if they don't know about that, you know, device security, just touching on that. We talk about the average person would think an antivirus is important. Antivirus is a reactive technology. We have it in place, but it's really of not a great importance. We're looking at things of being proactive. So being reactive is largely too late.

So there's a number of technologies that we use in terms of managed detection response. It's looking at these are platforms that have fully monitored 24/7 from, from a number of teams that are looking at processes that are occurring, that shouldn't be occurring. Like if someone's got access to a mailbox and they're putting in place, you know, forwarding within a mailbox to a certain

folder so that the user can't see certain communications from a hacker and things with a supplier or client.

These platforms are looking at all of that and alerting people like us. And I don't want to scare people off. These platforms have become a hell of a lot more affordable these days and we generally, you know, if you look at a provider like us, we bundle in all the support, IT support, day-to-day support and security and what have you into a user per month fee, and that's come down a hell of a lot over recent years. And that's another important one is support. Generally, like everybody, but particularly strata managers, if something is not right IT wise, whether it's hardware or software or a range of things, they need support now and they need it now, not waiting days and days and days. So we pride ourselves on that, as should any IT provider, because it's gone to the days where you can wait you know, many, many hours or days or weeks to get something fixed. So that's vitally important. And of course, seven days a week, we're finding that people have flexible working hours, they're working at 7 am in the morning, they're working at 7pm at night or later, and they're working Saturdays and Sundays and being flexible around family and what have you. So we're adapting to that. And so does the cyber security. We've had to adapt to that because it's not a wait-till-Monday type scenario. Something happens on a Saturday morning or a Friday night. It's gotta be looked at there and then.

Amanda Farmer

For sure. You've mentioned there, Tom, Microsoft and Windows and most people in this area using those platforms. I have noticed that too in the legal profession, I'm one of those odd people who actually does use a Mac and I use Gmail and Google Workspace.

What does that mean for me? Am I more exposed? Is Microsoft the better platform to be using?

Tom Buckley

Oh, look, no. And it's what you're comfortable in using and what works for you and your industry and what have you. I mean, I focus on Microsoft because that's where the bulk of the industry sits. I mean, if we haven't done the numbers recently, but it'd be well into the 90s in terms of who's using what. Google, obviously the second biggest player in the market and obviously Mac from a hardware perspective, there's certainly things, you know, the old age old age old adage of Macs being not vulnerable is a bit of a fallacy. They do and they looked about so that manage detection response we put on devices, making sure they're compliant with updates and etc., so there's a number of things there that we look at and it's absolutely critical because they do have the vulnerabilities and you've also got to think that there's a number of programs that are sitting with it on the Mac. For example, people do use Microsoft Office and a number of video conferencing platforms and things. And that's a good one because it has been some vulnerabilities in terms of those software, which makes then the device vulnerable.

In terms of Google, there is a number of things there that you should be doing in terms of the way that the Google Workspace in organization is set up. So in securing those, and again, all that area that I mentioned in regards to the domain security is provider agnostic. So the technical jargon I use DMARK, DKIM and SPF and all this stuff it may not mean a lot to people but that is relevant to your domain and making sure it's secure as possible. We can do very quick analysis on a domain, and we get this information publicly as to how secure our domain is and I can run that within about 30 seconds and tell someone just how secure they are.

So that it's looking at those things and so it's, there's no right or wrong in terms of the platforms you use, but they all come with a lot of security features, but generally not a lot turned on. Very rarely does it come turned on because they can't turn these on because every user, every organization, the platforms they use are nuanced to their requirements. If they just turn all this stuff on then you know the world wouldn't work. It needs a lot of modification and manipulation to make sure it's right for each user and organization.

Amanda Farmer

Well, now that everybody is suitably terrified, where can they go to find out more, Tom, to make sure that they are protected or better protected and that their clients are also? Where can they go to connect with you? Find out more about Strata IT.

Tom Buckley

Yes, for sure. I suppose our website is the best point of contact to call us to email us to submit a web form at stratait.com.au. So stratait.com.au and you know, we're happy to engage with people to do an analysis to see where they're at. You know, we're quite

Publication Date: 27 July 2023

YSP Podcast Transcript: 372. What are YOU doing about cyber security?

relaxed in terms of our engagement. We're not pushing in any regard. We're super passionate about IT. We're IT geeks at heart, but we're you know, common sense and try to provide it in as plain English as possible with all of our team and, you know, and obviously know the strata industries and its nuances. So if you're concerned or you just want better support, you know, a lot of people come to us just for better IT support, day-to-day IT support, parking the cyber security or aside, you know, they're coming to us for "How do I get all of our programs working in harmony better?", you know, "What are the people doing that we should be doing?" There are a lot of those questions we get also, so we're willing to take people through that journey as well.

Amanda Farmer

And you serve clients, right across Australia?

Tom Buckley

Yes, we serve everyone on what we call the Eastern Seaboard. So, Sunshine Coast, Brisbane, Gold Coast, we've got a Northern Rivers office in Byron Bay, Sydney, Melbourne, and out in we've also got a base in the central west of New South Wales. There are office locations, but we work with people, again, all across Australia. We've got access and people generally in all the capital cities nearly weekly. So it's you know, we can do 95% of our job remotely, but it is important to engage with people and be on site. So we're strong believers in that, but yeah, we've got a presence in most of the nooks and crannies of Australia.

Amanda Farmer

Excellent. Well, thank you so much for spending time with us today and sharing what it is that you do, what it is that our strata managers can be doing, should be thinking about when it comes to their IT and particularly cyber security in this day and age. I'll make sure that the link to your website is in the show notes for this episode and look forward to catching up with you again soon.

Tom Buckley

Awesome. Thanks, Amanda.

Outro: Thank you for listening to Your Strata Property, the podcast which consistently delivers to property owners, reliable and accurate information about their strata property. You can access all the information below this episode via the show notes at yourstrataproperty.com.au.